

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY**

STOCKROOM, INC.,

Plaintiff,

VS.

DYDACOMP DEVELOPMENT CORP.,
and PLUG & PAY TECHNOLOGIES,
INC.,

Defendants.

Case No: 2:11-cv-06220-WHW-SCM

**PLAINTIFF’S BRIEF IN OPPOSITION TO DEFENDANT DYDACOMP
DEVELOPMENT CORP.’S MOTION TO DISMISS THE SECONDAMENDED
COMPLAINT**

Vincent S. Verdiramo, Esq.
(VSV0830)
Verdiramo & Verdiramo, P.A.
3163 Kennedy Boulevard
Jersey City, New Jersey 07306
(201) 798-7082
(201) 798-4627 - fax
verdiramo@aol.com
Attorneys for Plaintiff

TABLE OF CONTENTS

Table of Authorities.....	iii
I. Introduction.....	1
II. Discussion.....	2
A. Software Defect Litigation Requires Flexibility In Applications Of Legal Rules And Doctrines Created Before Computers Even Existed.....	2
B. Plaintiff Has Alleged Several Breaches Of Contract That Are Within The 4-Year Limitations Period.....	4
C. Equitable Tolling Applies To Plaintiff's Contractual / Warranty Claims.....	5
1. Pleading Requirements For Equitable Tolling.....	5
a. Elements Of Equitable Tolling.....	5
b. When The Defendant Controls The Evidence Of Fraud, The Specificity Pleading Requirement Is Relaxed.....	7
2. The SAC Adequately Pleads Fraudulent Conduct And Concealment.....	9
3. Stockroom Has Met Its Pleading Burden.....	12
a. Dydacomp's Fraudulent Acts And Concealment.....	12
b. The Fraud Allegations Meet Rule 9(b)'s Specificity Requirements.....	14
c. The Cases Dydacomp Cites Are Distinguishable.....	14
d. Plaintiff Has Adequately Pled Its Fraud-Based Claims.....	17
1. Plaintiff Has Alleged Facts Supporting Fraud With The Requisite Specificity.....	17
2. Plaintiff Has Adequately Alleged Aggravating Circumstances To State A Claim Under New Jersey's Consumer Fraud Act.....	18

3. The Breach Of Fiduciary Duty Claim.....	21
III. CONCLUSION.....	22

TABLE OF AUTHORITIES

Principles Of The Law Of Software Contracts.....	3, 4
NJSA 12A:2-725.....	4
N.J.S.A.56:8-1 et seq.....	18
Rule 9(b).....	8
Rule 12(b)(6).....	6
UCC 2-725.....	6
<u>Burlington Coat Factory Securities Litigation</u> , 114 F. 3d 1410 (3d Cir. 1997)..	7
<u>Christidis v. First Pennsylvania Mortg. Trust</u> , 717 F.2d 96, 99-100 (3d Cir. 1983).	8
<u>Community Bank of Northern Virginia</u> , 467 F. Supp. 2d 466 (W.D. Pa 2006).....	15
<u>Cox v. Sears Roebuck & Co.</u> , 647 A. 2d 454 (NJ 1994).....	20
<u>Craftmatic Sec. Litig.</u> , 890 F.2d 628, 645 (3d Cir.1989).....	8
<u>Dewey v. Volkswagem AG</u> , 558 F.Supp. 2d 505, 523 (D.N.J. 2008).....	5
<u>Dunn v. Borough of Mountainside</u> , 301 NJ Super. 262, 280 (App. Div. 1997), cert. den. 153 NJ 402 (1998).....	5, 6
<u>F.D.I.C. v. Bathgate</u> , 27 F.3d 850, 876 (3d Cir.1994).....	9
<u>Foodtown v. Sigma Mktg Sys., Inc.</u> , 518 F. Supp. 485, 488 (D.N.J.1980).....	6
<u>Ford Motor Co. E-350 Van Products Liability Litigation (No. II)</u> , 2008 WL 4126264, *18 (D.N.J.).	13, 14
<u>Ford Motor Co. Ignition Switch Products Liability Litigation</u> , 1999 WL 33495352, *11 (D.N.J.), opinion vacated in part, 1999 WL 34824273 (1999)..	7
<u>Friedman v. Friendly Ice Cream Co.</u> , 133 N.J.Super., 333 (App. Div. 1975).....	5
<u>Galvao v. GR Robert Const. Co.</u> , 179 N.J. 462, 473, 846 A. 2d 1215 (2004).....	12
<u>Gardner v. Rosecliff Realty Co.</u> , 4 N.J. Super 1, 9, 124 A. 2d 30 (NJ App. Div. 1956).....	13
<u>Gutierrez v. TD Bank</u> , 2102 U.S. Dist.LEXIS, 29-30 (D.N.J. Jan 27,2012).....	15

<u>Hundred East Credit Corp. v. Eric Shuster Corp.</u> , 212 N.J.Super. 350 (App. Div. 1986).....	17
<u>Lerch v. Citizens First Bancorp., Inc.</u> , 805 F.Supp. 1142, 1152 (D.N.J. 1992).....	8
<u>Palmucci v. Brunswick Corp.</u> , 710 A. 2d 1045 (NJ App. Div. 1998).....	20
<u>Poskin v. TD Banknorth, N.A.</u> , 687 F.Supp. 2d 530, 550 (3d Cir. 2009).....	14, 15
<u>Price v. New Jersey Mfrs. Ins. Co.</u> , 368 NJ Super. 356, 362-363 (App. Div. 2004), aff'd 182 N.J.519 (2005).....	5
<u>Rockefeller Center Properties, Inc.</u> , 311 F. 3d 198, 216 (3d Cir. 2002).....	7
<u>Roth v. First Nat'l State Bank</u> , 169 N.J.Super. 280, 285, 404 A.2d 1 182 (App.Div.), cert. den., 81 N.J. 338, 407 A.2d 1212 (1979).....	12
<u>Saturn L-Series Timing Chain Products Liability Litigation</u> , 2008 WL 4866604, *7 (D.Neb.).....	6,7
<u>Statler v. Dell, Inc.</u> , 775 F. Supp. 2d 474, 483 (E.D.N.Y. 2011)	6
<u>Suber v. Chrysler Corp.</u> , 104 F.3d 578 (3d Cir. 1997).....	21
<u>Villalobos v. Fava</u> , 775 A. 2d 700, 707 (N.J. App. Div. 2001), cert. denied, 170 N.J. 210 (2001).....	5

I. INTRODUCTION

Dydacomp's motion to dismiss is based almost entirely on the assertion that Plaintiff Stockroom has failed to adequately plead an act of fraud to support its claims for equitable tolling and statutory and common law fraud. In making this argument, Dydacomp ignores express allegations in the second amended complaint ("SAC") and asks seemingly rhetorical questions that ignore the specific facts and circumstances in this case.

Stockroom's claims are based on an error in Dydacomp's Mail Order Manager ("MOM") software that caused the issuance of fake credit card authorization codes without communicating with the merchant bank. Stockroom lost more than \$600,000. Stockroom has alleged that the faulty software programming at issue could only have been intentional and knowing, and that faulty programming was therefore fraudulent. This was not an error that goes part-and-parcel with necessary programming. This was an error that was specifically created to make the program do something it was never supposed to do: issue dummy credit card authorizations without communicating with the merchant banks to get real approval. The program never should have been able to do this. This type of programming could only be a knowing and intentional act. No other explanation is possible. While Dydacomp controls the details as to who, what, where, why and when this happened such that Stockroom cannot make more specific allegations at this time, one thing is clear: fraud had to be involved in the creation of the faulty programming and the concealment of that fault. Dydacomp is responsible for its programmers' intentional acts. And case law is crystal clear that when the fraud evidence is exclusively in the Defendant's control, specificity is excused.

The misrepresentations consisted of statements in promotional and sales materials stating that the MOM software processed credit card transactions. Billions of credit card transactions

are processed daily, and the authorization code is indispensable to instantaneous transactions that fuel our consumer economy. Representing that the software processed credit card transactions includes an intrinsic representation that the software will not issue dummy authorization codes. The dummy authorization codes themselves were also misrepresentations. The authorization codes were representations that a financial transaction had processed. But for eleven years 3.2% of Stockroom's financial transactions were not properly processed or processed at all.

Dydacomp recites selective facts and acts incredulous that it took so long to discover the problem. But this is feigned; Dydacomp knows and was counting on the fact that retailers never audit to determine if authorization codes are correct. It would put too much of a burden on retailers and commerce; consumers would eventually have to pay for such additional auditing costs in product costs. Because of the differing schedules on which merchant banks deposit funds, deduct fees and credit refunds, the only way to determine if authorization codes are correct is to actually close bank accounts. This would be a huge burden on retailers, and by extension, commerce. No retailer does this.

Stockroom has more than adequately alleged fraudulent acts and concealment, and its breach of contract and warranty claims are equitably tolled. Additionally, these allegations support the fraud-based claims, and those must survive as well.

II. DISCUSSION

A. Software Defect Litigation Requires Flexibility In Applications Of Legal Rules And Doctrines Created Before Computers Even Existed

This case is based on defects in a software program that performed functions it should never have been able to. Most of the legal doctrines that apply to this case were created long before software even existed, passed without consideration or anticipation of the Computer Age

and the resulting legal issues that would arise in our courts. Recently, in 2010, the American Law Institute published Principles Of The Law Of Software Contracts (“ALI Principles”).

These Principles seek to clarify and unify the law of software transactions. In light of the many percolating legal issues that pertain to the formation and enforcement of software agreements, an attempt to “restate” this law would be premature. Reinforcing this view, software technology continues to develop, which influences methods of doing business and changes or creates new legal issues. [Citation]. Instead of restating the law, a “Principles” project accounts for the case law and recommends best practices, without unduly hindering the law's adaptability to future developments.

The introduction spells out the formidable issues:

The law of software transactions continues to develop. Case law and secondary literature present unresolved issues concerning (1) the nature of software transactions; (2) the lawfulness of current practices of contract formation and the implications of these practices for determining governing terms; . . . and (4) the appropriateness of contract terms concerning quality, remedies, and other rights. Because of its burgeoning importance, perhaps no other commercial subject matter is in greater need of harmonization and clarification. [Citation]. Although the software industry is relatively young, it constitutes an increasingly important share of our economy. [Citation]. Further, the law governing the transfer of hard goods is inadequate to govern software transactions because, unlike hard goods, software is characterized by novel speed, copying, and storage capabilities, and new inspection, monitoring, and quality challenges. [Citation]. In short, parties to software transactions would greatly benefit from the clarification and improvement of this area of the law. Software transferors and copyholders of all types can perform their various roles confidently and efficiently only after the clarification of applicable rules.

ALI Principles, Introduction. Section 3.05 sets forth the following rules: “(a) Unless modified or excluded, implied warranties may arise from course of dealing or usage of trade.” This includes warranties based on trade practice. (Cmt. a). (b) a software seller “warrants that the software contains no material hidden defects of which the transferor was aware at the time of the transfer. This warranty may not be excluded. In addition, this warranty does not displace an action for misrepresentation or its remedies.” (Cmt. b).

“Subsection (b) . . . memorializes existing law, including the contract obligation of good faith, the contract duty to disclose, and fraudulent-concealment law.” (Cmt b).

“A *hidden* material defect means that the defect would not surface upon any testing that was or should have been performed by the transferee. . . . As with fraudulent-concealment law, ordinarily § 3.05(b) should require an intent to deceive, which may be inferred if a transferor licenses software it knows is materially defective and knows the user cannot discover it upon an inspection.” *Id.* “Software transferors should have a duty to disclose known material hidden defects in order to allocate those risks to the party best able to accommodate or avoid them. Hidden material defects, known to the software transferor but not disclosed, shift costs to the transferee who cannot learn of the defects until it is too late and therefore cannot protect itself.” *Id.*

The ALI Principles and situations cited above exactly fit the facts of this case. While New Jersey law is applicable and Plaintiff has met its burden to maintain its SAC, the law should be applied with the understanding that these software issues are somewhat uncharted territory. Stockroom paid tens of thousands of dollars for the software and to process its credit card transactions. It expected an industry standard product that would not issue fake authorization codes and it had no reasonable way to detect the faulty programming. Under the circumstances, Dydacomp’s knowing distribution of the software with the defect is actionable.

B. Plaintiff Has Alleged Several Breaches Of Contract That Are Within The 4-Year Limitations Period

A four-year limitations period applies to the breach of contract and breach of warranty claims. NJSA 12A:2-725. This action was filed on October 21, 2011. (Dkt. 1). Thus, any breaches occurring from October 22, 2007 are within the limitations period. The original

software was installed in 1999. (SAC, ¶ 9, Ex. A). But several upgrades and versions were installed from in or about the first quarter of 2008 and thereafter. (SAC, ¶ 9). The license agreements related to those installs are set forth as Exhibits B-G. Because these contracts were entered within the limitations period, the claims for breach of those agreements were timely made within the limitations period.

C. Equitable Tolling Applies To Plaintiff's Contractual / Warranty Claims

1. Pleading Requirements For Equitable Tolling

a. Elements Of Equitable Tolling

As to the original contract (Ex. A), equitable tolling applies. As the Court noted in its opinion granting the motion to dismiss the amended complaint, for tolling, Plaintiff must plead “(1) wrongful concealment . . . resulting in (2) plaintiff’s failure to discover the operative facts forming the basis of his cause of action during the limitations period (3) despite exercise of due diligence.” (Dkt 30 at 7, *quoting, Dewey v. Volkswagern AG*, 558 F.Supp. 2d 505, 523 (D.N.J. 2008)). The doctrine of equitable tolling is available “when a plaintiff is misled . . . and as a result fails to act within the prescribed time limit.” *Villalobos v. Fava*, 775 A. 2d 700, 707 (N.J. App. Div. 2001), *cert. denied*, 170 N.J. 210 (2001) . “Equitable tolling affords relief from inflexible, harsh or unfair application of a statute of limitations.” *Id.* at 708.

The doctrine may be applied if one party has concealed or withheld information from the other causing the missing of a deadline. *Villalobos, supra*, at 50. *Friedman v. Friendly Ice Cream Co.*, 133 N.J.Super., 333 (App. Div. 1975), *Price v. New Jersey Mfrs. Ins. Co.*, 368 NJ Super. 356, 362-363 (App. Div. 2004), *aff'd* 182 N.J.519 (2005). A statute of limitations cannot be used “as a sword” by an adversary whose misconduct prevents a claimant from filing within the limitation period. *Dunn v. Borough of Mountainside*, 301 NJ Super. 262, 280 (App. Div.

1997), *cert. den.* 153 NJ 402 (1998). The doctrine has been applied numerous times to avoid the strictures of UCC 2-725. *See Foodtown v. Sigma Mktg Sys., Inc.*, 518 F. Supp. 485, 488 (D.N.J.1980) and cases cited therein.

Jurisdictions other than New Jersey have also held that a plaintiff may invoke equitable tolling to avoid the unfair application of the four-year statute of limitations in the UCC's Section 2-725. Many have dismissed motions to dismiss under Rule 12(b)(6) because the motions were premature when critical facts the plaintiffs needed to establish equitable tolling could only be later determined through discovery or otherwise. For example, one New York court held:

While Plaintiff's amended complaint details ongoing problems with his Optiplex computers, it does not state, with any precision, when those problems began, or the dates of service by Dell. Additionally, the court is in no position, at this stage of the proceedings, to make factual findings with respect to Dell's conduct. Discovery will uncover facts regarding Dell's conduct, as well as those that may ultimately support the conclusion that Plaintiff possessed more than enough information to commence a timely lawsuit. Such a conclusion cannot be reached, however, only upon consideration of the pleadings and other documents before the court on this motion. Accordingly, the court will not rule, at this time, whether equitable principles can toll the running of the statute of limitations, or estop Defendant from asserting a statute of limitations defense. The court therefore denies the motion to dismiss the warranty claims at this time. Such claims may or may not be saved by equitable tolling; *it is simply too early to tell.*

Statler v. Dell, Inc., 775 F. Supp. 2d 474, 483 (E.D.N.Y. 2011) (emphasis added). Similarly, another federal court in an unreported case, refused to dismiss breach of implied warranty claims as time barred, stating:

Because it is clear from the Complaint that Plaintiffs' claims ordinarily would be time-barred by the statute of limitations, *at trial* Plaintiffs will bear the burden of demonstrating to the trier of fact the Defendants' alleged fraudulent acts of concealment. If Plaintiffs fail to persuade the trier of fact that Defendants fraudulently concealed their products' defects, Plaintiffs' implied warranty claims will be barred by the statute of limitations as a matter of law. *To dismiss these claims at this stage in the proceedings would be improper.*"

In re Saturn L-Series Timing Chain Products Liability Litigation, 2008 WL 4866604, *7

(D.Neb.) (emphasis added).

Similarly, a New Jersey District Court denied a 12(b)(6) defendant auto manufacturer's motion by seeking a dismissal under UCC 2-725. *In re Ford Motor Co. Ignition Switch Products Liability Litigation*, 1999 WL 33495352, *11 (D.N.J.), *opinion vacated in part*, 1999 WL 34824273 (1999). The plaintiffs alleged that Ford knew or should have known of defects in its ignition switch and the court found that the plaintiffs could not possibly have discovered their causes of action against Ford until a federal agency began an investigation of ignition-switch related fires years after many of the plaintiffs' purchases. The court held:

Accordingly, the court holds that the applicable statutes of limitations were tolled under the doctrine of fraudulent concealment until NHTSA initiated its initial investigation of ignition switch-related fires in August 1992. . . and, therefore, denies Ford's motion for judgment on the pleadings on plaintiffs' implied warranty claims on the grounds that plaintiffs' claims are time-barred.

Id. at*11.

b. When The Defendant Controls The Evidence Of Fraud, The Specificity Pleading Requirement Is Relaxed

With respect to the fraud allegations required to equitable tolling, to comply with Rule 9(b), specific allegations are not necessary when the information is not available. "Where it can be shown that the requisite factual information is peculiarly within the defendant's knowledge or control, the rigid requirements of Rule 9(b) may be relaxed. *Id.* Nevertheless, even when the defendant retains control over the flow of information, '*boilerplate and conclusory allegations will not suffice. Plaintiffs must accompany their legal theory with factual allegations that make their theoretically viable claim plausible.*'" *In re Rockefeller Center Properties, Inc.*, 311 F. 3d 198, 216 (3d Cir. 2002), *quoting, In re Burlington Coat Factory Securities Litigation*, 114 F. 3d 1410 (3d Cir. 1997) (emphasis in original). The Third Circuit explains the origin and pleading

requirements of Rule 9(b):

Historically, Rule 9(b) is derived from English common law practice. See C. Clark, Code Pleading § 48, at 312 (2d ed. 1947); English Rules for the Supreme Court under the Judicature Act, Order 19, Rule 6, The Annual Practice (1937). As Judge Clark noted:

[i]t has been the rule under both common-law and code pleading that allegations of fraud must be made with a great degree of particularity. Thus, it is said that the elements of fraud in an action for false representation are five, as follows: (1) A specific false representation of material facts; (2) knowledge by the person who made it of its falsity; (3) ignorance of its falsity by the person to whom it was made; (4) the intention that it should be acted upon; and (5) the plaintiff acted upon it to his damage. C. Clark, Code Pleading § 48, at 312 (2d ed. 1947). It is the identification of these elements of a fraud claim which the first sentence of Rule 9(b) requires. The rule applies not only to fraud actions under federal statutes, but to fraud claims based on state law. In applying the first sentence of Rule 9(b) courts must be sensitive to the fact that its application, prior to discovery, may permit sophisticated defrauders to successfully conceal the details of their fraud. Moreover, in applying the rule, focusing exclusively on its “particularity” language “is too narrow an approach and fails to take account of the general simplicity and flexibility contemplated by the rules.” 5 C. Wright & A. Miller, Federal Practice and Procedure § 1298, at 407 (1969).

Christidis v. First Pennsylvania Mortg. Trust 717 F.2d 96, 99-100 (3d Cir. 1983); *see also*, *Lerch v. Citizens First Bancorp., Inc.*, 805 F.Supp. 1142, 1152 (D.N.J. 1992) (where information necessary to prove fraud claim is within defendant corporation's control, a plaintiff may satisfy rule of pleading fraud with particularity by stating how plaintiff attempted to gain necessary information to plead fraud more particularly and that the defendant has exclusive control over necessary information). The reason for the rule is that “in cases such as corporate fraud, a plaintiff ‘cannot be expected to have personal knowledge of the details of corporate internal affairs’ and thus has ‘relaxed the rule when factual information is peculiarly within the defendant's knowledge or control.” *In re Craftmatic Sec. Litig.*, 890 F.2d 628, 645 (3d Cir.1989). However, in such circumstances, the plaintiff must expressly allege that the necessary

information lies within the defendant's exclusive control and provide facts sufficient to indicate that the charges are not baseless. *Id*; *F.D.I.C. v. Bathgate*, 27 F.3d 850, 876 (3d Cir.1994).

2. The SAC Adequately Pleads Fraudulent Conduct And Concealment

The SAC allegations meet the equitable tolling pleading burden. Dydacomp represented in sales and promotional materials that its software processed credit card transactions. (SAC, ¶ 8). Credit card processing includes the issuance of authorization codes, which are universally recognized as a confirmation that the customer's credit card would be charged for a transaction so that, in Stockroom's case, product was shipped. In essence, the code is a statement of fact the retailer relies upon as establishing the legitimacy of the transaction. (SAC, ¶ 15).

Dydacomp designs and sells the MOM software, which, among other things, processes credit card transactions. Until recently, Stockroom used MOM and Defendant Plug & Pay's processing gateway to process its credit card transactions. In mid-2010, Stockroom discovered by happenstance that the merchant banks were not paying Stockroom some of the proceeds from credit card sales. After several months of trying to get to the bottom of the problem with Dydacomp, Stockroom was finally able to get enough cooperation to retrieve some of the data necessary to analyze the problem. Through that audit, Stockroom discovered that it was not paid for about three percent (3%) of its credit card transactions each year. To make matters worse, several credit card refunds that Stockroom issued were credited back more than once. One refund was credited to the customer *nineteen times*. All told, Stockroom has lost at least several hundred thousand dollars. Authorization codes were communicated in every transaction. (SAC, ¶¶ 19; 33).

Stockroom only discovered that it had lost money when it closed a retail store in 2010 and the bank accounts for that store. This created an end-point for transactions, and when all the

card issuers had completed their deposits of sale proceeds and withdrawal of fees, Stockroom was able to determine for the first time that it had lost money. Before that, detection would have been impossible because of the varying deposit and fee withdrawal schedules of the merchant banks and the timing of chargebacks and refunds. Some months the problematic transactions were only 2 out of every 1,000 transactions; other months there were more (as high as 8%). The average problematic transactions were about three percent overall. (SAC, ¶¶ 18-21).

Stockroom did not catch the problem earlier because it was basically impossible to audit the records for evidence of dummy authorization codes.

Retailers throughout the world rely on the understanding that receipt of an authorization code means that the funds will be deposited to the retailer's merchant bank account. Retailers routinely rely on receipt of an authorization code to send out product or perform services. Plaintiff therefore reasonably relied on the authorization codes generated by DydaComp in this case as validation of the subject transactions. There is no generally accepted or routine accounting practice whereby audits are conducted to ensure that credit card authorization codes are valid and that funds are accurately debited or credited based on receipt of an authorization code. Such audits would take a substantial amount of time and would be fruitless because of the varied schedule of deposits, fees and chargebacks. The only way to get an accurate reading would be to change bank accounts each time an audit is performed. The audit would take a substantial amount of time, and changing bank accounts would as well. Few if any companies routinely do this to determine or confirm whether authorization codes are valid and such extraordinary actions are outside the scope of ordinary due diligence.

(SAC, ¶ 22).

There is no expectation that online retailers will audit their financial records to determine the validity of the authorization codes. On the contrary, merchants routinely and absolutely rely on the authorization codes to release product or perform services before receiving the funds because that is the stated purpose of authorization codes. Software providers such as DydaComp must have adequate protocols in place to ensure against dummy authorization codes or credits of

the same refunds multiple times. Dydacomp's competitors take such steps as a routine matter and would never expect its customers to be able to catch such problems. (SAC, ¶¶ 23, 24).

After extensive internal auditing and communications with Dydacomp and Plug & Pay, Stockroom determined that Dydacomp's software likely caused the problem. Plug & Pay informed Stockroom that it appeared that Dydacomp was issuing the authorization codes improperly. According to Plug & Pay, when a transaction is entered through the M.O.M. system, the M.O.M. software is supposed to contact Plug & Pay's system to get an authorization code approving or denying the transaction. M.O.M. is supposed to get the authorization code from Plug & Pay, which receives the code from the merchant bank. The authorization is never supposed to originate with Dydacomp or M.O.M. under any circumstance, ever. In all cases, the authorization code must come from the financial institution that is ultimately responsible for approving the transaction. Plug & Pay informed Stockroom that for the faulty transactions it reviewed, there was absolutely no communication between the M.O.M. software and Plug & Pay. Plug & Pay suggested that based on the lack of communication, the M.O.M. software never initiated the communication and just issued the authorization codes itself, without asking for or, by extension, waiting for a code to come back from the merchant bank through Plug & Pay. Additionally, several of the authorization codes were identical. The odds of having repeated instances of identical authorization codes are prohibitively low. Furthermore, the odds that such extraordinary results could have happened randomly without knowledge on Dydacomp's part are even lower. Although Dydacomp denied that M.O.M. was the source of the problem, in fact it is impossible for the M.O.M. software to issue an authorization code without being programmed to do so. The M.O.M. software is never supposed to issue an authorization code and indeed should not have the ability to do so. Each authorization code was thus a misrepresentation regarding the status of the transaction.

(SAC, ¶ 31).

Stockroom alleges on information and belief that one or more agents of Dydacomp knew of the problems with M.O.M.'s issuance of dummy authorization codes without communication with the gateway. Rather than fix the problem with the original software sold to Stockroom, or thereafter in upgrades or new software concealed the problem with the software from Stockroom. **Under the circumstances, it is not possible for a programmer or software developer to have been unaware of the problem. Somebody intentionally created the software code that caused the M.O.M. software to independently generate the authorization codes and return those illegitimate codes back to Stockroom. The entire transaction approval process requires complex and intentional software coding. It does not happen by accident or glitch in the software.**

(SAC, ¶ 32, emphasis added).

Using reasonable diligence, Stockroom could not have reasonably discovered the problem earlier than June 2010. The problem was discovered only because Stockroom closed the bank account for the Stormy Leather retail store in San Francisco. Otherwise, it is impossible to track and compare revenue to actual gross sales because the merchant banks deposit the charged funds at different times. Sometimes it is the same day; sometimes the next day, and sometimes it is a few days later. Visa and Mastercard charge their fees once a month; American Express, every day. Thus, all such calculations would always be at least a few thousand dollars off. Moreover, Stockroom did not feel the need to audit to ensure full payment on the credit card transactions because authorization codes were issued, and Stockroom had no reason to doubt that it would get paid on those approved transactions.

(SAC, ¶ 34).

3. Stockroom Has Met Its Pleading Burden

a. Dydacomp's Fraudulent Acts And Concealment

Stockroom has alleged specific facts sufficient to plead equitable tolling. Specifically, the emboldened language, above, makes clear that this could not have been an accident. The faulty code had to be created by a programmer, who knew that it was faulty. And, at the very least, the programmer, Dydacomp's agent, then concealed the error. (The programmer may have communicated this fault to others at Dydacomp who also then concealed the defects). These are two different acts: intentional faulty programming and concealment of that faulty programming.

An employer is vicariously liable for tortious conduct of an employee that is within the scope of his employment. *Galvao v. GR Robert Const. Co.*, 179 N.J. 462, 473, 846 A. 2d 1215 (2004). An employee's conduct within the scope of employment when "it is of the kind that he is employed to perform; it occurs substantially within the authorized time and space limits; [and] it is actuated, at least in part, by a motivation to serve the master." *Roth v. First Nat'l State Bank*, 169 N.J. Super. 280, 285, 404 A.2d 1182 (App.Div.), *cert. den.*, 81 N.J. 338, 407 A.2d 1212 (1979). Moreover, "a principal may be held, in an action of deceit, for damages resulting from his agent's fraudulent representation, where the principal has put the agent in such a position that

a person of ordinary prudence, conversant with business uses, would be justified in presuming that the agent has the authority to make the representation.” *Gardner v. Rosecliff Realty Co.*, 4 N.J. Super 1, 9, 124 A. 2d 30 (NJ App. Div. 1956). Thus, Dydacomp is liable for its employees’ and agents’ fraud.

In addition, each fake or dummy authorization code was a misrepresentation that the software worked properly and furthered the concealment. The promotional materials representing that the software processed credit card transactions contained an intrinsic representation / assumption that authorization codes issued would be legitimate and reliable. The sales materials concealed the fact that the software could issue dummy or fake codes without communicating with the gateway to the merchant banks.

Given the liberality with which pleadings are treated at this stage in the lawsuit, the bar is not usually very high. In another case, Ford claimed that the plaintiffs had not sufficiently pled the elements of fraudulent concealment in support of their claim for equitable tolling. The court responded:

Although Plaintiffs could have done so with greater precision, this Court finds that for the purposes of withstanding a motion to dismiss, Plaintiffs have sufficiently pled reliance on Defendant’s alleged misrepresentation and omissions. Notably, in the Complaint, Plaintiffs allege that Defendant’s conduct constituted acts of “deception, fraud, false pretenses, false promises, misrepresentation and/or a knowing concealment, suppression, or omission of material facts with the intent that Plaintiffs . . . would *rely* upon such concealment, suppression, or omission in connection with the sale, marketing, advertisement and subsequently performance of the E350 van.”

In re Ford Motor Co. E-350 Van Products Liability Litigation (No. II), 2008 WL 4126264, *18 (D.N.J.). The language used in that case is remarkably similar to Plaintiff’s allegation in this case. In addition to the allegation that only fraud could have caused the defect in this case and that Dydacomp actively concealed it in sales and promotional materials and in subsequent

upgrades and issuances of fake authorization codes. Furthermore, Plaintiff has accused Defendants of “deception, fraud, false pretense, false promise or misrepresentation”, words virtually identical to those approved of by the court in *Ford Motor, supra*. (SAC, ¶ 58). Some facts concerning Defendant’s behavior relevant to equitable tolling will have to await discovery, however, as noted in some of the cases cited above.

b. The Fraud Allegations Meet Rule 9(b)’s Specificity Requirements

The SAC meets Rule 9(b) specificity requirements. Stockroom has pled as many facts as it could. The remaining facts are in Dydacomp’s control. Stockroom has also alleged that it did all it could to learn more about the fraud and exercised reasonable diligence under the unique circumstances of this case. As soon as the retail store account closed and Stockroom noticed the problem, Stockroom began investigating and auditing. Stockroom spent several months trying to get information from Dydacomp, who was not helpful and did not offer any explanation. Stockroom knows there was a fraud because the defect in the software is evidence of fraud. Stockroom knows that the software did not process credit card transactions as represented in sales and promotional materials and Stockroom knows that dummy authorization codes were issued in 3.2% of its transactions, which codes were also misrepresentations. Stockroom has alleged that Dydacomp controls the rest of the information regarding the fraud and concealment thereof. Under the circumstances, Stockroom has pled its fraud claims and equitable tolling with the requisite specificity.

c. The Cases Dydacomp Cites Are Distinguishable

The cases Dydacomp cites are distinguishable. All three were lender liability cases in which there was no evidence of concealment of fraudulent loan terms beyond the initial provision of the loan documents to the plaintiffs. In *Poskin v. TD Banknorth, N.A.*, 687 F.Supp.

2d 530, 550 (3d Cir. 2009), plaintiffs alleged that loan documents did not contain the loan terms they believed they had agreed to and that one of the defendants involved had repeatedly ignored requests for the correct loan documents. But another defendant had provided the actual loan documentation, and plaintiffs waited past the running of the statute of limitations to sue. The court ruled that equitable tolling did not apply because although one defendant had not responded to a request for the loan documents, another had and thus the plaintiffs had the information they needed to proceed to suit. *Poskin* is distinguishable from this case because in this case, Plaintiff had no knowledge or means of finding out about the dummy authorization codes.

In *Gutierrez v. TD Bank*, 2102 U.S. Dist.LEXIS, 29-30 (D.N.J. Jan 27,2012), the plaintiffs brought a class action against a lender for mortgage-related wrongs and alleged that their claims were equitably tolled because they were fraudulently induced to take the loans. But the court ruled that equitable tolling did not apply because there was no act beyond the initial fraudulent act to invoke equitable tolling. In that case, the plaintiffs had not even attempted to discover the fraud by requesting information or protesting payments. Accordingly, there was no basis for equitable tolling.

In *In Re Community Bank of Northern Virginia*, 467 F. Supp. 2d 466 (W.D. Pa 2006), the misrepresentations at issue were contained in the loan documents given to the plaintiffs when the loans originated. There was no further attempt or even opportunity to conceal the alleged frauds – they were right in the loan documents.

In contrast, in this case, the fraudulent acts at issue were the intentional programming that allowed the dummy authorization codes to be originated, the concealment of the existence of the faulty programming as evidenced by representations in sales and promotional materials that the

software processed credit card transactions. Authorization codes are indispensable components to credit card transactions. Intrinsic in those sales and promotional materials was a representation that Stockroom could rely on the authorization codes that would be issued with each transaction that it would be paid for sale or that a refund would be issued only one time. Moreover, each authorization code was a separate representation that Dydacomp knew was false.

Dydacomp required Stockroom to use Plug & Pay and if Stockroom wanted to use the M.O.M. software to process transactions, it had to use Plug & Pay. Presumably, the reason Dydacomp required that Stockroom use Plug & Pay is because Dydacomp received a portion of the fees Stockroom paid to Plug & Pay, which was a minimum of \$25 per month and eight cents per transaction. (SAC, Ex. H). This added up to thousands of dollars each month in gateway fees alone. Moreover, Dydacomp charged thousands of dollars for each upgrade. Dydacomp thus profited from continuing to conceal the defect in its program. This is not a situation where the fraudulent act was a one-time thing and then the defendant just stayed silent. Dydacomp actively required Stockroom to pay for upgrades by threatening to jeopardize Stockroom's ability to process credit card transactions – its livelihood. Moreover, it profited each time a transaction was processed. Dydacomp knew that its program was faulty and failed to disclose it to preserve its continuing ability to profit from upgrades and each and every transaction processed.

Dydacomp's argument that faulty programming in and of itself could not create and inference of fraud evidences that Dydacomp misses the point of the fraudulent act alleged here. Dydacomp argues that all products are intentionally created by their manufacturer and if a product winds up containing a faulty part, it is not necessarily evidence of fraud. This is true. Certainly an engineer could forget to think of an issue in designing a product and this is not intentional. But Defendant's premise does not apply to the software programming and the defect

in this case. A programmer had to intentionally create a way for the software to issue dummy authorization codes. The programmer had to know that it was intentionally putting a defect in the product and then either concealed it - a concealment for which Dydacomp is liable as the principal of the programmer - or the programmer revealed it to others and they participated in the concealment. Either way, Stockroom is alleging that in this particular case, under the circumstances, only fraud could be involved.

Stockroom has adequately alleged the elements of equitable tolling. Dydacomp controls all other information available regarding the circumstances of the fraud, and thus Stockroom has met its pleading burden and its breach of contract / warranty claims should not be dismissed.

D. Plaintiff Has Adequately Pled Its Fraud-Based Claims

1. Plaintiff Has Alleged Facts Supporting Fraud With The Requisite Specificity

Dydacomp asserts that Stockroom has failed to adequately plead its claims under the New Jersey Consumer Fraud Act (“CFA”) and common law fraud. As set forth above, Plaintiff has met the Rule 9(b) pleading standards. Plaintiff alleges that the only possible way for the software at issue to have the ability to issue dummy authorization codes is if somebody intentionally programmed the software to do that. This wasn’t a random error; it was intentional. And then Dydacomp marketed and promoted the software and forced Stockroom to buy upgrades, and to use Plug & Pay as the communication gateway to the merchant banks.

This case is similar to the situation in *Hundred East Credit Corp. v. Eric Shuster Corp.* 212 N.J.Super. 350 (App. Div. 1986). The plaintiff purchased a “P-142 disc unit and a P-143 disc drive (peripherals) to expand the capacity of a P-359 computer . . .” *Id* at 352. Commenting on the plaintiff’s status as a corporation, the court noted:

Business entities, like individual consumers, cover a wide range. Some are poor, some wealthy; some are naive, some sophisticated; some are required to submit,

some are able to dominate. Even the most world-wise business entity can be inexperienced and uninformed in a given consumer transaction. Unlawful practices thus can victimize business entities as well as individual consumers. It may well be, of course, that certain practices unlawful in a sale of personal goods to an individual consumer would not be held unlawful in a transaction between particular business entities; the Act largely permits the meaning of “unlawful practice” to be determined on a case-by-case basis.

Id at 356-7. As in the case at bar, defendant's wrong was one of nondisclosure of material information:

[T]he trial judge found that at the time of the 1976 sales Philips knew that production of the P-350 line of computers, including the P-359, “would end some time in 1976” but nevertheless “continued to market and sell the computers ... in an organized, systematic plan to liquidate the inventory of P-350 line computers so as to avoid sustaining a loss of profits on these items.” The judge further found that at the time Philips sold the peripherals neither Schuster nor the “consuming public” had been informed of the imminent discontinuance of the P-350 line. Discontinuing manufacture of the P-350 series in 1976 meant that Schuster was “unable to accomplish the objectives which motivated its purchases in the first instance.” The judge concluded that Philips' conduct was fraudulent and also constituted “unconscionable commercial practices” within the meaning of N.J.S.A. 56:8-2. *Id* at 353-4

The appellate court affirmed the trial court's findings of fact and affirmed, but reduced the judgment against the defendant under the CFA. The specifics of how the faulty programming occurred are within DydaComp's specific control, and therefore it is not necessary to plead those specifics to survive the pleading stage for the CFA and common law fraud claims. *See* discussion in Sections II-C-1-b and 3-b, above.

2. **Plaintiff Has Adequately Alleged Aggravating Circumstances To State A Claim Under New Jersey's Consumer Fraud Act**

Defendant contends that Plaintiff has failed to plead substantial aggravating factors to state a cause of action for consumer fraud under N.J.S.A.56:8-1 et seq., maintaining that all that was pled was that Defendant breached implied and express warranties. This is clearly not so.

Stockroom alleges that only by intentional acts could the software have been caused to

issue dummy authorization codes, something it should NEVER have been able to do, given the stakes. Moreover, Dydacomp, knowing of this defect, nevertheless promoted the software as being able to process credit card transactions, forced Stockroom to buy upgrades and to use Plug & Pay to process transactions, from which Dydacomp received money from Plug & Pay. Plaintiff alleges that based on these facts, Defendant has engaged in “an unconscionable commercial practice, deception, fraud, false pretense, false promise or misrepresentation. . . .” against the Plaintiff. (SAC, ¶ 58). Plaintiff further alleges that Dydacomp “knowingly concealed, suppressed, or omitted a material fact from Stockroom with the intent that Stockroom rely upon same.” (SAC, ¶ 58). Moreover, Dydacomp did not in good faith assist Plaintiff in trying to get at the source of the problem, dragging its feet and denying culpability. (SAC, ¶¶ 28, 29). When Plaintiff was finally able to perform a limited audit, it appeared that the MOM software was issuing authorization codes on its own, and not getting the codes from the merchant banks as it was supposed to. Some of these codes were identical, which is almost statistically impossible. (SAC, ¶ 31). To the extent that Plaintiff relied on these false authorization codes to ship products, the issuance of these codes amounted to deception, fraud, false pretense, false promise or misrepresentation. The allegations of these paragraphs are incorporated by reference into the CFA claim. (SAC, ¶ 54).

Furthermore, considering what has been learned to date, Plaintiff is highly skeptical, given the volume of transactions Dydacomp's promotional material on its website and elsewhere claims it is involved in, that Plaintiff's case is the first time this problem has surfaced. If other customers discovered and complained about this problem previously and Dydacomp made no effort to warn Plaintiff and to seek to repair the problem, then Plaintiff contends that such nondisclosure amounted to fraudulent concealment, consistent with the FAC

allegations, and an unconscionable business practice. Plaintiff intends to serve discovery to uncover just how much Defendant knew (or should have known) about this problem while it purported to deal with Plaintiff in good faith. Defendant would like to give the Court the impression that its dealings with Plaintiff all occurred in the “last century.” In fact, however, after the initial sale, Defendant required Plaintiff to purchase several upgrades, over a period of years, the last such one occurring in 2010. Plaintiff is prepared to show that each such upgrade was a separate purchase involving, in each instance, the purchase and delivery of a new software disk. Plaintiff believes that, at sometime during the years these transactions were occurring, Defendant received actual notice of the defects in its system.

The cases Dydacomp cites are distinguishable. In *Palmucci v. Brunswick Corp.*, 710 A. 2d 1045 (NJ App. Div. 1998), the court held that the fact “the defendant had an internal policy determining when it will replace an entire engine cannot equate with an unconscionable business practice. Under its warranty, Brunswick had the right to repair or replace as it chose. It had the discretion to repair when it wished to do so or to replace an entire engine if it elected to do so.” *Id.* at 1049. In contrast, in this case, Dydacomp (or its agents) intentionally caused a defect in the software that never should have been there in the first place, and then actively concealed the defect in marketing materials and thousands of transactions upon which Stockroom justifiably relied.

Dydacomp cites *Cox v. Sears Roebuck & Co.*, 647 A. 2d 454 (NJ 1994) for the proposition that a breach of warranty cannot form the basis for a CFA claim. In that case, the New Jersey Supreme Court held that there was no evidence of “any bad faith or lack of fair dealing on the part of Sears” and thus the breach of contract in that case did not “rise to the level of an ‘unconscionable commercial practice’ in violation of the Act. *Id.* at 20. In this case,

Stockroom has alleged an unconscionable commercial practice: an intentional defect in the software, misrepresentations that continued with each issuance of a fake authorization code and active concealment.

Although the facts are distinguishable, the *Cox* Court laid out the standards for determining if an unlawful practice exists under the CFA: “To violate the Act, a person must commit an “unlawful practice” as defined in the legislation. Unlawful practices fall into three general categories: affirmative acts, knowing omissions, and regulation violations.” *Id.* at 17. When the alleged consumer-fraud violation consists of an affirmative act, intent is not an essential element and the plaintiff need not prove that the defendant intended to commit an unlawful act. [Citation omitted]. However, when the alleged consumer fraud consists of an omission, the plaintiff must show that the defendant acted with knowledge, and intent is an essential element of the fraud. [Citation omitted].” *Id.* at 18. *See also, Suber v. Chrysler Corp.*, 104 F.3d 578 (3d Cir. 1997) (finding that allegations supported finding of substantial aggravating circumstances in addition to breach of warranty).

Stockroom meets both standards. The affirmative act was the intentional programming of the software to issue authorization codes without communicating with the gateway. The omission consisted of the promotions and sales materials stating that the software processes credit card transactions, and the issuance of each fake authorization code on an ongoing basis.

3. The Breach Of Fiduciary Duty Claim

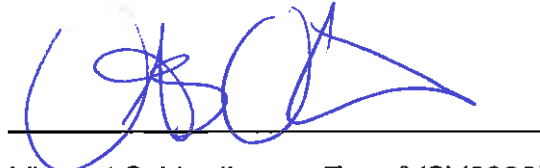
Stockroom agrees to dismiss its claim for breach of fiduciary duty.

III.

CONCLUSION

For all the foregoing reasons, Plaintiff respectfully requests that the Court deny Defendant Dydacomp's motion to dismiss.

Dated: January 3, 2013



Vincent S. Verdiramo, Esq. (VSV0830)

Verdiramo & Verdiramo, P.A.

3163 Kennedy Boulevard

Jersey City, New Jersey 07306

201-798-7082, 201-798-4627 (fax)

verdiramo@aol.com